Received: 07 October 2022 | Accepted: 25 June 2024 | Published Online: 29 June 2024

Recoletos Multidisciplinary Research Journal Vol. 12 no. 1 (June 2024)

DOI: https://doi.org/10.32871/rmrj2412.01.12

RECOLETOS
MULTIDISCIPLINARY RESEARCH JOURNAL

Almost Difference Sets from Unions of Cyclotomic Classes of Order 10

Benedict Estrella

Mathematics Department,
College of Science, Bulacan State
University, Bulacan, Philippines

*Correspondence:
benedict.estrella@bulsu.edu.ph

Abstract

This study investigated the problem of constructing almost difference sets from single and unions of cyclotomic classes of order 10 (with and without zero) of the finite field GF(q), where q is a prime of the form q = 10n+1 for integer n≥1 and q<1000. Using exhaustive computer searches in Python, the method computed unions of two classes up to nine cyclotomic classes. Moreover, the equivalence of the generated almost difference sets having the same parameters was determined up to complementation. Results showed that a single cyclotomic class formed an almost difference set for q = 31, 71, and 151, while including zero produced an almost difference set for q=11, 31, 71, and 151. Additionally, Paley partial difference sets were constructed from the union of five cyclotomic classes. These findings addressed gaps in the literature on cyclotomy of order 10.

Keywords

almost difference set, cyclotomic class, union

INTRODUCTION

According to a survey on almost difference sets by Nowak (2014) and Ding et al. (2014), the study of almost difference sets is of interest in combinatorics and have a wide range of applications in engineering such as CDMA communications, coding theory and cryptography. In CDMA communications, some cyclic almost difference sets yield sequences having optimal autocorrelation. The original motivation for introducing and studying almost difference sets is the construction of binary sequences with optimal autocorrelation (Ding, 2014). Likewise, in coding theory, they can be employed to construct cyclic codes. Lastly, in cryptography, they can be used to construct functions with optimal nonlinearity.

Let $(G,+)$ be an abelian group of order q. A k-subset D of G is a (q,k,λ,t) almost difference set of G if the difference function $\mathrm{diff}_D(x)$ takes on λ altogether t times and $\lambda+1$ altogether $q-1-t$ times when x ranges over all the nonzero elements of G, where the difference function $\mathrm{diff}_D(x)$ is given by $\mathrm{diff}_D(x) = |D \cap (D+x)|$. This definition is adopted by Ding et al. (2001), which is a generalization and a unified version of the two definitions of almost difference sets introduced in

Davis (1992) and Ding (1994). The study notes that almost difference sets are just generalizations of difference sets when $t = 0$ or $t = q - 1$. Throughout this paper, the author only considers almost difference sets with $t \neq 0$ and $t \neq q - 1$.

Cyclotomy is a powerful tool for constructing almost difference sets where cyclotomic classes of finite fields are employed. Moreover, there are very few constructions of almost difference sets from unions of cyclotomic classes. In the literature, cyclotomic classes of orders 2, 4, 8, and 12 were employed to construct almost difference sets but no constructions from unions of cyclotomic classes of order 10. It would be interesting if new constructions could be found.

In this paper, the author shows new construction of cyclotomic almost difference sets from unions of suitable cyclotomic classes of order 10 (with and without the residue zero) of the finite field $GF(q)$, where q is a prime of the form $q = 10n + 1$ for integer $n \geq 1$ using an exhaustive computer search.

METHODS

Preliminaries

An almost difference set D is called abelian or cyclic (nonabelian or noncyclic) if the group G is abelian or cyclic (nonabelian or noncyclic). Two almost difference sets D_1 and D_2 are considered equivalent if there exists an automorphism σ of G and an element $b \in G$ such that $\sigma(D_1) = D_2 + b$. In particular, if G is cyclic, D_1 and D_2 are equivalent if an integer a with $\gcd(a, q) = 1$ exists, such that $aD_1 = D_2 + b$ for some $b \in G$ (Ding et al., 2014).

If D is a (q, k, λ, t) almost difference set in an abelian group $(G, +)$, then $k(k-1) = t\lambda + (q - 1 - t)(\lambda + 1)$. Moreover, its complement, $D^C = G \setminus D$ is also an almost difference set in $(G, +)$ with parameters $(q, q - k, q - 2k + \lambda, t)$ (Ding, 2014).

A classical method for constructing almost difference sets in the additive groups of finite fields is to use cyclotomic classes of finite fields. Let $q = nN + 1$ be a power of a prime, and let α be a fixed primitive element of $GF(q)$. Define ${C_i}^{(N,q)} := \alpha^i \langle \alpha^N \rangle$, where $\langle \alpha^N \rangle$ denotes the multiplicative group generated by α^N. The cosets ${C_i}^{(N,q)}$ are called the cyclotomic classes of order N in $GF(q)$ (Ding et al., 2014).

The theorem below summarizes some known almost difference sets constructed via cyclotomy (Ding, 2014; Nowak, 2014) .

Theorem 2.1: Below is a list of cyclotomic almost difference sets in $(GF(q), +)$.

1. ${C_0}^{(2,q)}$ with parameters $(q, (q-1)/2\,, (q-5)/4, (q-1)/2)$, where $q \equiv 1 \pmod 4$. It is also called the Paley partial difference set.
2. ${C_0}^{(4,q)}$ with parameters $(q, (q-1)/4, (q-13)/16, (q-1)/2)$, where $q = 4t^2 + 25$ or $q = 4t^2 + 9$ and t^2 is odd.
3. ${C_0}^{(4,q)} \cup \{0\}$ with parameters $(q, (q+3)/4, (q-5)/16, (q-1)/2)$, where $q = 4t^2 + 1$ or $q = 4t^2 + 49$ and t^2 is odd.
4. ${C_0}^{(4,q)} \cup {C_1}^{(4,q)}$ with parameters $(q, (q-1)/2, (q-5)/4, (q-1)/2)$, where $q = t^2 + 4$ and $t \equiv 1 \pmod 4$.
5. ${C_2}^{(4,q)} \cup \{0\}$with parameters $(q, (q+3)/4, (q-5)/16, (q-1)/2)$, where $q = 4t^2 + 1$ or $q = 4t^2 + 49$ and t is odd.

6. ${C_0}^{(8,q)}$ with parameters $(q,(q-1)/8,(q-41)/64,(q-1)/2)$, where $q \equiv 41 \pmod{64}$ and $q = 4t^2 + 19^2 = 2b^2 + 1$ for some integer t and b or $q \equiv 41 \pmod{64}$ and $q = 4t^2 + 13^2 = 2b^2 + 1$ for some integer t and b.
7. ${C_0}^{(8,q)} \cup \{0\}$ with parameters $(q,(q+7)/8,(q-9)/64,3(q-1)/4)$, where $q = 64t^2 + 9 = 8b^2 + 1$ for some odd integers t and b

The following theorem indicates that unions of cyclotomic classes of order eight can be employed to construct almost difference sets (Ding et al., 2014).

Theorem 2.2: Suppose that $r = t^2 + 2 \equiv 3 \pmod{8}$ is a prime power, where t is an integer. Let $q = r^2$. Then the set $D = {C_0}^{(8,q)} \cup {C_1}^{(8,q)} \cup {C_2}^{(8,q)} \cup {C_5}^{(8,q)}$ is an almost difference set in $(GF(q),+)$ with parameters $(q,(q-1)/2,(q-5)/4,\ (q-1)/2)$, provided that the generator α of $GF(q)^*$ employed to define the cyclotomic classes of order eight is appropriately chosen.

The following theorem shows that unions of cyclotomic classes of order 12 can be employed to construct almost difference sets (Nowak et al., 2013).

Theorem 2.3: Let q be a prime of the form $q = t^2 + 4 \equiv 1 \pmod{12}$, where $t \equiv 1 \pmod{4}$. Then the set $D = {C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_5}^{(12,q)} \cup {C_8}^{(12,q)} \cup {C_9}^{(12,q)}$ is an almost difference set in $(GF(q),+)$ with parameters $(q,(q-1)/2,(q-5)/4,\ (q-1)/2)$ for an adequately chosen primitive element of $GF(q)$ employed to define the cyclotomic classes of order 12.

Ma included the following result in his survey of partial difference sets, which produces a lot of almost difference sets in $(GF(q\ ),+)$, where q is an even power of a prime (Ding, 2014).

Theorem 2.4: Assume that p is an odd prime, $N \geq 2$ is a positive even integer, $q = p^{2jy}$, where $N|\ (p^j + 1)$ for some j and j is the smallest such positive integer. If $y, p, \frac{p^j+1}{N}$ are all odd, then the set $D = \sum_{i \in I} {C_i}^{(N,q)}$ is a $(q,(q-1)/2,(q-5)/4,(q-1)/2)$ almost difference set in $(GF(q),+)$, where these ${C_i}^{(N,q)}$ are cyclotomic classes of order N in $GF(q)$, and $I \ \subset \{0,1,\dots,N-1\}$ with $|I| = N/2$.

Computational Procedure

The computational procedure adopted the search method from the algorithms of Balmaceda & Estrella (2021) and Estrella (2022). Given an input prime q, the method finds all almost difference sets from unions of two or more GF(q) cyclotomic classes with or without zero. The search was performed for all primes $q < 1000$ of the form $q = 10n + 1$. Lastly, it was determined whether the obtained almost difference sets, if any, are equivalent to each other and to known cyclotomic almost difference sets, as described in Theorem 2.1, Theorem 2.2, Theorem 2.3, and Theorem 2.4.

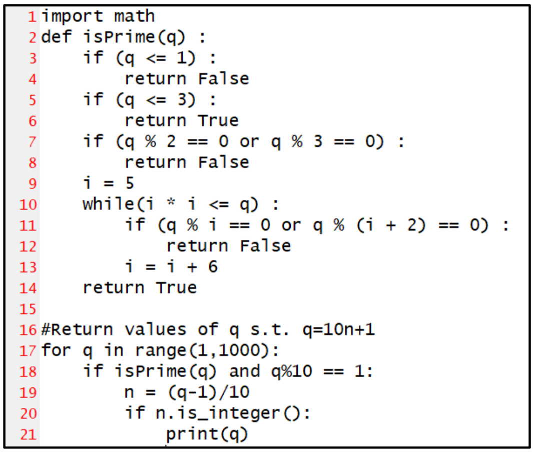
Computer programs were written using Python, performing the following steps for a given input q.

1. Choose a primitive element α of $GF(q)$.
2. Compute the cyclotomic classes ${C_i}^{(10,\,q)}$ using the chosen primitive element.
3. Take the union of ${C_0}^{(10,q)}$ with a second cyclotomic class and test if the obtained set forms an almost difference set.
4. If no almost difference set is found, repeat steps 1–3 using a different primitive element until an almost difference set is obtained or until the primitive elements of $GF(q)$ are exhausted.
5. Repeat steps 1–4 using the union of ${C_0}^{(10,q)}$ with another cyclotomic class until all unions of ${C_0}^{(10,q)}$ with a second cyclotomic class are exhausted.
6. Repeat steps 1–5, using ${C_0}^{(10,q)}$ with two other cyclotomic classes, then ${C_0}^{(10,q)}$ with three other cyclotomic classes, and so on up to ${C_0}^{(10,q)}$ with eight other cyclotomic classes.

7. For each almost difference set obtained, check its equivalence with other generated sets with the same parameters and to known cyclotomic difference sets.

The same steps will be applied but include zero in the unions to search for other possible cyclotomic almost difference sets.

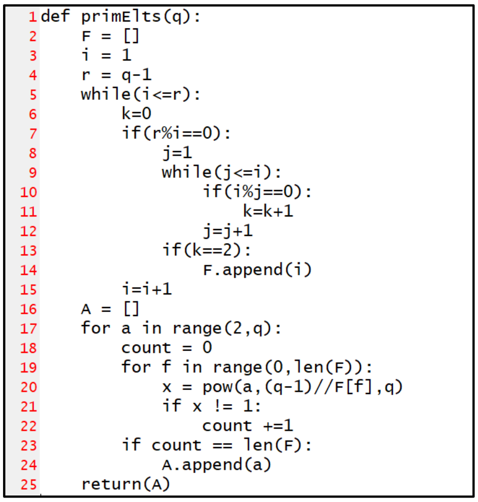
To find all primes $q < 1000$ of the form $10n + 1$ where n is any integer, the following code in Figure 1 was utilized. Lines 2-14 will determine if the number q is prime or not. Lines 17-21 will return all prime numbers less than 1000, congruent to 1 modulo 10.



```
 1 import math
 2 def isPrime(q) :
 3     if (q <= 1) :
 4         return False
 5     if (q <= 3) :
 6         return True
 7     if (q % 2 == 0 or q % 3 == 0) :
 8         return False
 9     i = 5
10     while(i * i <= q) :
11         if (q % i == 0 or q % (i + 2) == 0) :
12             return False
13         i = i + 6
14     return True
15 
16 #Return values of q s.t. q=10n+1
17 for q in range(1,1000):
18     if isPrime(q) and q%10 == 1:
19         n = (q-1)/10
20         if n.is_integer():
21             print(q)
```

Figure 1. *Prime Numbers of the Form* $10n + 1$

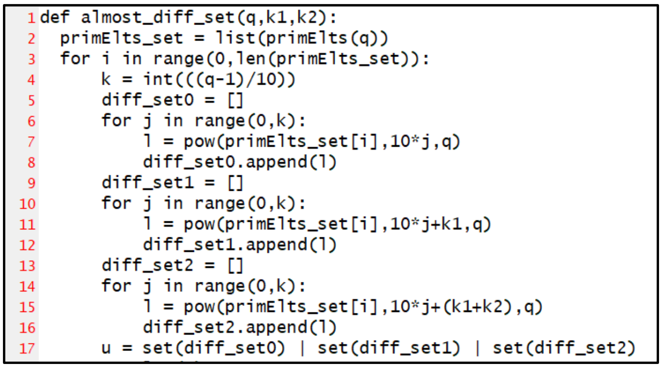
Figure 2 shows the defined function $primElts(q)$ to determine all primitive elements of $GF(q)$ for each input prime q. These primitive elements are used to define the cyclotomic classes of order 10.



```
def primElts(q):
    F = []
    i = 1
    r = q-1
    while(i<=r):
        k=0
        if(r%i==0):
            j=1
            while(j<=i):
                if(i%j==0):
                    k=k+1
                j=j+1
            if(k==2):
                F.append(i)
        i=i+1
    A = []
    for a in range(2,q):
        count = 0
        for f in range(0,len(F)):
            x = pow(a,(q-1)//F[f],q)
            if x != 1:
                count +=1
        if count == len(F):
            A.append(a)
    return(A)
```

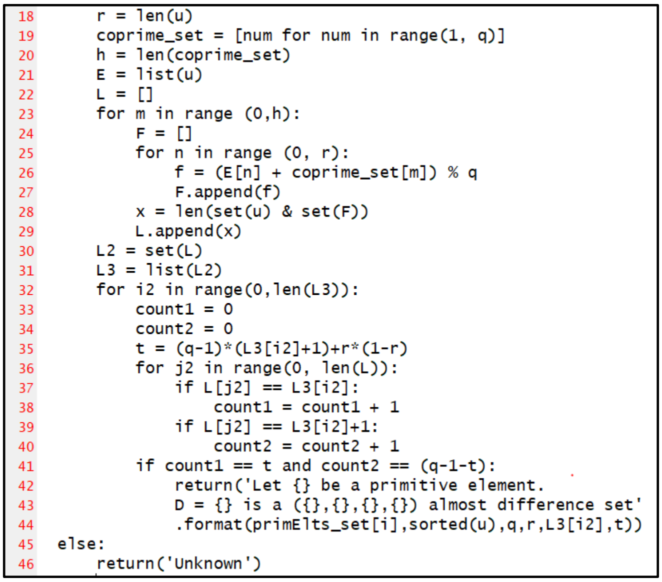
Figure 2. *Primitive Elements*

Next, another function, $almost\_diff\_set(parameters)$, was defined to determine the existence of almost different sets from unions of two cyclotomic classes up to unions of nine classes. The case of three cyclotomic classes was discussed, as shown in Figures 3 and 4. The classes can be represented by ${C_0}^{(10,q)} \cup {C_{i_1}}^{(10,q)} \cup {C_{i_2}}^{(10,q)}$ where $1 \leq i_1 < i_2 \leq 9$. From Figure 3, the set of all primitive elements was computed using the function $primElts(q)$ in line 2. In line 3, the program identified the first primitive element in the list to compute the cyclotomic classes in lines 4-16. The obtained union in line 17 was subjected to codes in lines 32-44 of Figure 4 to check if it formed an almost difference set. If no almost difference set was found, the program took the next primitive element. Using the second primitive element, the cyclotomic classes were again computed. Then, the same union was considered and tested for the existence of almost difference set. The same steps were repeated until an almost different set existed or the primitive elements of $GF(q)$ were all exhausted. The same procedure was applied until the possible unions of three classes were exhausted.



```
1 def almost_diff_set(q,k1,k2):
2    primElts_set = list(primElts(q))
3    for i in range(0,len(primElts_set)):
4        k = int(((q-1)/10))
5        diff_set0 = []
6        for j in range(0,k):
7            l = pow(primElts_set[i],10*j,q)
8            diff_set0.append(l)
9        diff_set1 = []
10       for j in range(0,k):
11           l = pow(primElts_set[i],10*j+k1,q)
12           diff_set1.append(l)
13       diff_set2 = []
14       for j in range(0,k):
15           l = pow(primElts_set[i],10*j+(k1+k2),q)
16           diff_set2.append(l)
17       u = set(diff_set0) | set(diff_set1) | set(diff_set2)
```

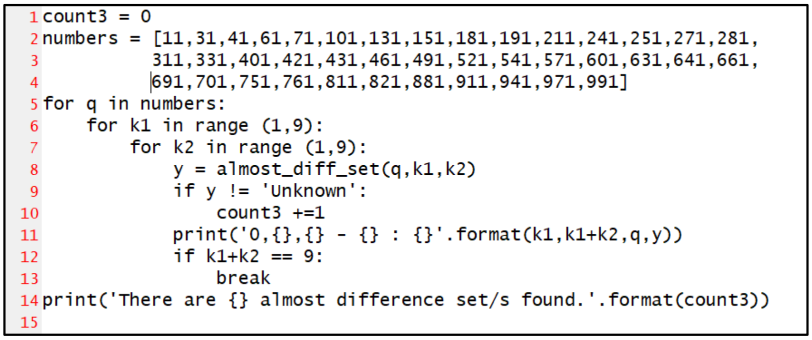
Figure 3. *Union of three cyclotomic classes*



```
18         r = len(u)
19         coprime_set = [num for num in range(1, q)]
20         h = len(coprime_set)
21         E = list(u)
22         L = []
23         for m in range (0,h):
24             F = []
25             for n in range (0, r):
26                 f = (E[n] + coprime_set[m]) % q
27                 F.append(f)
28             x = len(set(u) & set(F))
29             L.append(x)
30         L2 = set(L)
31         L3 = list(L2)
32         for i2 in range(0,len(L3)):
33             count1 = 0
34             count2 = 0
35             t = (q-1)*(L3[i2]+1)+r*(1-r)
36             for j2 in range(0, len(L)):
37                 if L[j2] == L3[i2]:
38                     count1 = count1 + 1
39                 if L[j2] == L3[i2]+1:
40                     count2 = count2 + 1
41             if count1 == t and count2 == (q-1-t):
42                 return('Let {} be a primitive element.
43                 D = {} is a ({},{},{},{}) almost difference set'
44                 .format(primElts_set[i],sorted(u),q,r,L3[i2],t))
45     else:
46         return('Unknown')
```

Figure 4. *Test for the existence of almost difference*

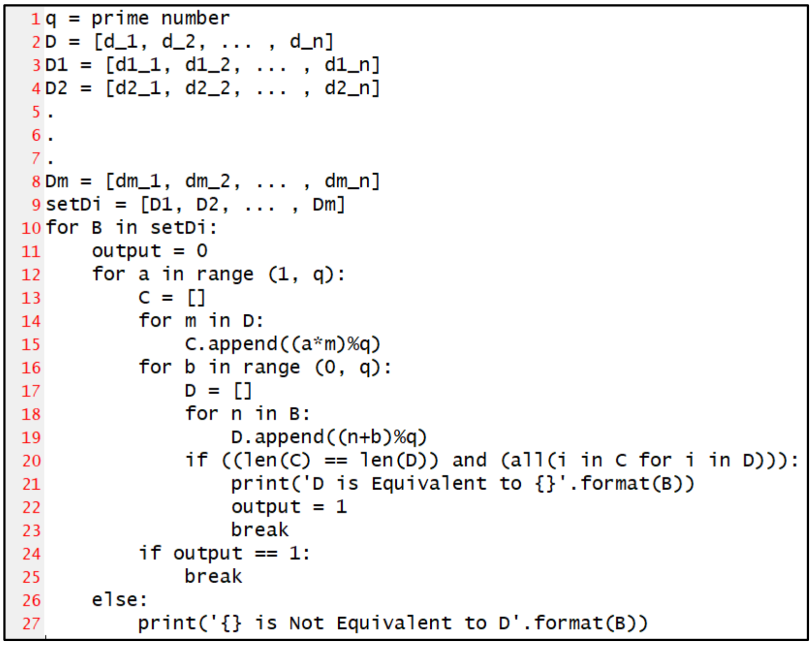
In addition, the codes in Figure 5 were needed to execute all the possible unions of three cyclotomic classes and test each prime $q < 1000$. In line 8, the function $almost\_diff\_set(q, k1, k2)$ was called to form the union and test the existence of almost difference sets.



```
 1 count3 = 0
 2 numbers = [11,31,41,61,71,101,131,151,181,191,211,241,251,271,281,
 3           311,331,401,421,431,461,491,521,541,571,601,631,641,661,
 4           691,701,751,761,811,821,881,911,941,971,991]
 5 for q in numbers:
 6     for k1 in range (1,9):
 7         for k2 in range (1,9):
 8             y = almost_diff_set(q,k1,k2)
 9             if y != 'Unknown':
10                 count3 +=1
11             print('0,{},{} - {} : {}'.format(k1,k1+k2,q,y))
12             if k1+k2 == 9:
13                 break
14 print('There are {} almost difference set/s found.'.format(count3))
15
```

Figure 5. *Test all possible unions for each q sets*

Finally, if there exist almost difference sets, the codes in Figure 6 will be run to test the equivalence of two or more almost difference sets with the same parameters.



```
q = prime number
D = [d_1, d_2, ... , d_n]
D1 = [d1_1, d1_2, ... , d1_n]
D2 = [d2_1, d2_2, ... , d2_n]
.
.
.
Dm = [dm_1, dm_2, ... , dm_n]
setDi = [D1, D2, ... , Dm]
for B in setDi:
    output = 0
    for a in range (1, q):
        C = []
        for m in D:
            C.append((a*m)%q)
        for b in range (0, q):
            D = []
            for n in B:
                D.append((n+b)%q)
            if ((len(C) == len(D)) and (all(i in C for i in D))):
                print('D is Equivalent to {}'.format(B))
                output = 1
                break
        if output == 1:
            break
    else:
        print('{} is Not Equivalent to D'.format(B))
```

Figure 6. *Test for Equivalence*

RESULTS AND DISCUSSION

Let $q < 1000$ be a prime of the form $q = 10n + 1$ for any integer $n \geq 1$. Table 1 summarizes the parameters (q, k, λ, t) and the unions of cyclotomic classes $C_i^{(10,q)}$ (with and without the residue zero), which form an almost difference set (up to equivalence) in the additive group $GF(q)$ for a suitably chosen primitive element of $GF(q)$ employed to define the cyclotomic classes of order 10.

Table 1. *Almost difference Sets from Cyclotomic Classes of Order 10 (up to equivalence)*

	$(\boldsymbol{q},\boldsymbol{k},\boldsymbol{\lambda},\boldsymbol{t})$	**Almost Difference Sets**
1	$(11,2,0,8)$	${C_0}^{(10,q)} \cup \{0\} = \{0,1\}$
		${C_0}^{(10,q)} \cup {C_i}^{(10,q)}$, for any i $(1 \le i \le 9)$
2	$(11,3,0,4)$	${C_0}^{(10,q)} \cup {C_i}^{(10,q)} \cup {C_j}^{(10,q)}$, for any i,j $(1 \le i \ne j \le 9)$
		${C_0}^{(10,q)} \cup {C_i}^{(10,q)} \cup \{0\}$, for any i $(1 \le i \le 9)$
3	$(11,4,1,8)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_3}^{(10,q)}$
		${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_3}^{(10,q)} \cup \{0\}$
4	$(11,7,4,8)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_3}^{(10,q)} \cup {C_4}^{(10,q)} \cup {C_5}^{(10,q)} \cup {C_7}^{(10,q)}$
		${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_3}^{(10,q)} \cup {C_4}^{(10,q)} \cup {C_5}^{(10,q)} \cup \{0\}$
5	$(11,8,5,4)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_3}^{(10,q)} \cup {C_4}^{(10,q)} \cup {C_5}^{(10,q)} \cup {C_6}^{(10,q)} \cup {C_7}^{(10,q)}$
		${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_3}^{(10,q)} \cup {C_4}^{(10,q)} \cup {C_5}^{(10,q)} \cup {C_6}^{(10,q)} \cup \{0\}$
6	$(11,9,7,8)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_3}^{(10,q)} \cup {C_4}^{(10,q)} \cup {C_5}^{(10,q)} \cup {C_6}^{(10,q)} \cup {C_7}^{(10,q)} \cup {C_8}^{(10,q)}$
		${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_3}^{(10,q)} \cup {C_4}^{(10,q)} \cup {C_5}^{(10,q)} \cup {C_6}^{(10,q)} \cup {C_7}^{(10,q)} \cup \{0\}$
7	$(31,3,0,24)$	${C_0}^{(10,q)} = \{1,5,25\}$
8	$(31,4,0,18)$	${C_0}^{(10,q)} \cup \{0\} = \{0,1,5,25\}$
9	$(31,7,1,18)$	${C_0}^{(10,q)} \cup {C_i}^{(10,q)} \cup \{0\}$, for any $i \in \{1,3,7,9\}$
10	$(31,7,1,18)$	${C_0}^{(10,q)} \cup {C_i}^{(10,q)} \cup \{0\}$, for any $i \in \{2,4,6,8\}$
11	$(31,9,2,18)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)}$
12	$(31,9,2,18)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_3}^{(10,q)}$
13	$(31,9,2,18)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_5}^{(10,q)}$
14	$(31,12,4,18)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_6}^{(10,q)}$
15	$(31,13,5,24)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_3}^{(10,q)} \cup \{0\}$
16	$(31,13,5,24)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_6}^{(10,q)} \cup \{0\}$
17	$(31,18,10,24)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_3}^{(10,q)} \cup {C_4}^{(10,q)} \cup {C_5}^{(10,q)}$
18	$(31,18,10,24)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_4}^{(10,q)} \cup {C_5}^{(10,q)} \cup {C_6}^{(10,q)}$
19	$(31,19,11,18)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_4}^{(10,q)} \cup {C_5}^{(10,q)} \cup {C_6}^{(10,q)} \cup \{0\}$
20	$(31,22,15,18)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_3}^{(10,q)} \cup {C_4}^{(10,q)} \cup {C_5}^{(10,q)} \cup {C_6}^{(10,q)} \cup \{0\}$
21	$(31,22,15,18)$	${C_0}^{(10,q)} \cup {C_1}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_3}^{(10,q)} \cup {C_4}^{(10,q)} \cup {C_5}^{(10,q)} \cup {C_7}^{(10,q)} \cup \{0\}$

Table 1. *(continued)*

	(q,k,λ,t)	**Almost Difference Sets**
22	$(31,22,15,18)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup C_5^{(10,q)} \cup C_6^{(10,q)} \cup C_7^{(10,q)} \cup \{0\}$
23	$(31,24,18,18)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup C_4^{(10,q)} \cup C_5^{(10,q)} \cup C_6^{(10,q)} \cup C_7^{(10,q)}$
24	$(31,24,18,18)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup C_4^{(10,q)} \cup C_5^{(10,q)} \cup C_6^{(10,q)} \cup C_8^{(10,q)}$
25	$(31,27,23,18)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup C_4^{(10,q)} \cup C_5^{(10,q)} \cup C_6^{(10,q)} \cup C_7^{(10,q)} \cup C_8^{(10,q)}$
26	$(31,28,25,24)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup C_4^{(10,q)} \cup C_5^{(10,q)} \cup C_6^{(10,q)} \cup C_7^{(10,q)} \cup C_8^{(10,q)} \cup \{0\}$
27	$(71,7,0,28)$	$C_0^{(10,q)} = \{1,20,30,32,37,45,48\}$
28	$(71,8,0,14)$	$C_0^{(10,q)} \cup \{0\} = \{0,1,20,30,32,37,45,48\}$
29	$(71,29,11,28)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_4^{(10,q)} \cup \{0\}$
30	$(71,42,24,28)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup C_4^{(10,q)} \cup C_6^{(10,q)}$
31	$(71,63,55,14)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup C_4^{(10,q)} \cup C_5^{(10,q)} \cup C_6^{(10,q)} \cup C_7^{(10,q)} \cup C_8^{(10,q)}$
32	$(71,64,57,28)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup C_4^{(10,q)} \cup C_5^{(10,q)} \cup C_6^{(10,q)} \cup C_7^{(10,q)} \cup C_8^{(10,q)} \cup \{0\}$
33	$(131,52,20,78)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_6^{(10,q)}$
34	$(131,53,21,104)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_6^{(10,q)} \cup \{0\}$
35	$(131,78,46,104)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_4^{(10,q)} \cup C_5^{(10,q)} \cup C_6^{(10,q)}$
36	$(131,79,47,78)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_4^{(10,q)} \cup C_5^{(10,q)} \cup C_6^{(10,q)} \cup \{0\}$
37	$(151,15,1,90)$	$C_0^{(10,q)} = \{1,2,4,8,16,19,32,38,59,64,76,85,105,118,128\}$
38	$(151,16,1,60)$	$C_0^{(10,q)} \cup \{0\}$ $= \{0,1,2,4,8,16,19,32,38,59,64,76,85,105,118,128\}$
39	$(151,135,120,60)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup C_4^{(10,q)} \cup C_5^{(10,q)} \cup C_6^{(10,q)} \cup C_7^{(10,q)} \cup C_8^{(10,q)}$
40	$(151,136,122,90)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup C_4^{(10,q)} \cup C_5^{(10,q)} \cup C_6^{(10,q)} \cup C_7^{(10,q)} \cup C_8^{(10,q)} \cup \{0\}$

The obtained almost difference sets in Table 1 are inequivalent with the known almost difference sets described in Theorem 2.1, Theorem 2.2, Theorem 2.3, and Theorem 2.4 since they have different parameters. A single cyclotomic class of order ten forms an almost difference set if $q = 31, 71, 151$. While a single cyclotomic class together with zero produces an almost difference set if $q = 11$, 31, 71, 151. There are two inequivalent $(31,7,1,18)$ almost difference sets generated from unions of two cyclotomic classes together with zero, three inequivalent $(31,9,2,18)$ almost difference sets generated from three cyclotomic classes, and two inequivalent $(31,13,5,24)$ almost difference sets generated from four cyclotomic classes together with zero. The researcher has observed that almost difference sets with parameters $(31,27,23,18)$, $(71,63,55,14)$, and $(151,135,120,60)$ can be generated from the same union of nine cyclotomic classes.

If one's attention is restricted to almost difference set D with $|D| \leq q/2$, the results are summarized in Table 2 up to complementation.

Table 2. *Almost difference Sets from Cyclotomic Classes of Order 10 (up to complementation)*

	(q, k, λ, t)	**Almost Difference Sets**
1	$(11, 2, 0, 8)$	$C_0^{(10,q)} \cup \{0\} = \{0, 1\}$
		$C_0^{(10,q)} \cup C_i^{(10,q)}$, for any i $(1 \leq i \leq 9)$
2	$(11, 3, 0, 4)$	$C_0^{(10,q)} \cup C_i^{(10,q)} \cup C_j^{(10,q)}$, for any i, j $(1 \leq i \neq j \leq 9)$
		$C_0^{(10,q)} \cup C_i^{(10,q)} \cup \{0\}$, for any i $(1 \leq i \leq 9)$
3	$(11, 4, 1, 8)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)}$
		$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_3^{(10,q)} \cup \{0\}$
4	$(31, 3, 0, 24)$	$C_0^{(10,q)} = \{1, 5, 25\}$
5	$(31, 4, 0, 18)$	$C_0^{(10,q)} \cup \{0\} = \{0, 1, 5, 25\}$
6	$(31, 7, 1, 18)$	$C_0^{(10,q)} \cup C_i^{(10,q)} \cup \{0\}$, for any $i \in \{1, 3, 7, 9\}$
7	$(31, 7, 1, 18)$	$C_0^{(10,q)} \cup C_i^{(10,q)} \cup \{0\}$, for any $i \in \{2, 4, 6, 8\}$
8	$(31, 9, 2, 18)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)}$
9	$(31, 9, 2, 18)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_3^{(10,q)}$
10	$(31, 9, 2, 18)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_5^{(10,q)}$
11	$(31, 12, 4, 18)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_6^{(10,q)}$
12	$(31, 13, 5, 24)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup \{0\}$
13	$(31, 13, 5, 24)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_6^{(10,q)} \cup \{0\}$
14	$(71, 7, 0, 28)$	$C_0^{(10,q)} = \{1, 20, 30, 32, 37, 45, 48\}$
15	$(71, 8, 0, 14)$	$C_0^{(10,q)} \cup \{0\} = \{0, 1, 20, 30, 32, 37, 45, 48\}$
16	$(71, 29, 11, 28)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_4^{(10,q)} \cup \{0\}$
17	$(131, 52, 20, 78)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_6^{(10,q)}$
18	$(131, 53, 21, 104)$	$C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_6^{(10,q)} \cup \{0\}$
19	$(151, 15, 1, 90)$	$C_0^{(10,q)} = \{1, 2, 4, 8, 16, 19, 32, 38, 59, 64, 76, 85, 105, 118, 128\}$
20	$(151, 16, 1, 60)$	$C_0^{(10,q)} \cup \{0\} = \{0, 1, 2, 4, 8, 16, 19, 32, 38, 59, 64, 76, 85, 105, 118, 128\}$

In addition, the set $D = C_0^{(10,q)} \cup C_2^{(10,q)} \cup C_4^{(10,q)} \cup C_6^{(10,q)} \cup C_8^{(10,q)}$ is an almost difference set in $(GF(q), +)$ with parameters $(q, (q-1)/2, (q-5)/4,\ (q-1)/2)$ where $q \equiv 1\ (mod\ 4)$. This set is equivalent to the Paley partial difference set. Similarly, the set $D = C_0^{(10,q)} \cup C_2^{(10,q)} \cup C_4^{(10,q)} \cup C_6^{(10,q)} \cup C_8^{(10,q)} \cup \{0\}$ is an almost difference set in $(GF(q), +)$ with parameters $(q, (q+1)/2, (q-1)/4,\ (q-1)/2)$ where $q \equiv 1\ (mod\ 4)$. This set is equivalent to the Paley partial difference set together with zero. The two constructions can generate infinitely many almost difference sets with such parameters in $(GF(q),+)$, for example, $q = 41, 61, 101, 181, 241, 281, 401, 421, 461, 521, 541, 601, 641, 661, 701, 761, 821, 881, 941\ldots$

The following are some examples of almost difference sets generated from unions of cyclotomic classes of order 10.

Example 3.1 Let $q = 31$ and let the primitive element $\alpha = 11$. Then

$$\begin{aligned} D &= C_0^{(10,q)} \cup C_1^{(10,q)} \cup \{0\} \\ &= \{0, 1, 5, 11, 24, 25, 27\} \end{aligned}$$

is a $(31, 7, 1, 18)$ almost difference set in $(GF(31),+)$.

Example 3.2 Let $q = 31$ and let the primitive element $\alpha = 11$. Then

$$\begin{aligned} D &= C_0^{(10,q)} \cup C_2^{(10,q)} \cup \{0\} \\ &= \{0, 1, 5, 16, 18, 25, 28\} \end{aligned}$$

is a $(31, 7, 1, 18)$ almost difference set in $(GF(31),+)$.

Example 3.3 Let $q = 31$ and let the primitive element $\alpha = 11$. Then

$$\begin{aligned} D &= C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \\ &= \{1, 5, 11, 16, 18, 24, 25, 27, 28\} \end{aligned}$$

is a $(31, 9, 2, 18)$ almost difference set in $(GF(31),+)$.

Example 3.4 Let $q = 31$ and let the primitive element $\alpha = 11$. Then

$$\begin{aligned} D &= C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_3^{(10,q)} \\ &= \{1, 5, 11, 12, 21, 24, 25, 27, 29\} \end{aligned}$$

is a $(31, 9, 2, 18)$ almost difference set in $(GF(31),+)$.

Example 3.5 Let $q = 31$ and let the primitive element $\alpha = 17$. Then

$$\begin{aligned} D &= C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_5^{(10,q)} \\ &= \{1, 5, 6, 17, 22, 23, 25, 26, 30\} \end{aligned}$$

is a $(31, 9, 2, 18)$ almost difference set in $(GF(31),+)$.

Example 3.6 Let $q = 31$ and let the primitive element $\alpha = 3$. Then

$$\begin{aligned} D &= C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup \{0\} \\ &= \{0, 1, 3, 5, 8, 9, 11, 13, 14, 15, 24, 25, 27\} \end{aligned}$$

is a $(31, 13, 5, 24)$ almost difference set in $(GF(31),+)$.

Example 3.7 Let $q = 31$ and let the primitive element $\alpha = 3$. Then

$$\begin{aligned} D &= C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_6^{(10,q)} \cup \{0\} \\ &= \{0, 1, 3, 5, 8, 9, 13, 14, 15, 16, 18, 25, 28\} \end{aligned}$$

is a $(31, 13, 5, 24)$ almost difference set in $(GF(31),+)$.

Example 3.8 Let $q = 31$ and let the primitive element $\alpha = 3$. Then

$$\begin{aligned} D &= C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_3^{(10,q)} \cup C_4^{(10,q)} \cup C_5^{(10,q)} \cup C_6^{(10,q)} \cup C_7^{(10,q)} \cup C_8^{(10,q)} \\ &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 28, 30\} \end{aligned}$$

is a $(31, 27, 23, 18)$ almost difference set in $(GF(31),+)$.

Example 3.9 Let $q = 31$ and let the primitive element $\alpha = 28$. Then

$$\begin{aligned} D &= C_0^{(10,q)} \cup C_1^{(10,q)} \cup C_2^{(10,q)} \cup C_4^{(10,q)} \cup \{0\} \\ &= \{0, 1, 2, 3, 4, 6, 9, 19, 20, 25, 28, 30, 32, 37, 38, 40, 42, 44, 45, 48, 49, 50, 53, 57, 59, \\ &\quad 60, 63, 64, 66\} \end{aligned}$$

is a $(71, 29, 11, 28)$ almost difference set in $(GF(71),+)$.

Example 3.10 Let $q = 41$ and let the primitive element $\alpha = 6$. Then
$D = {C_0}^{(10,q)} \cup {C_2}^{(10,q)} \cup {C_4}^{(10,q)} \cup {C_6}^{(10,q)} \cup {C_8}^{(10,q)}$
$= \{1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40\}$
is a $(41, 20, 9, 20)$ almost difference set in $(GF(41), +)$. This is equivalent to the Paley partial difference set.

CONCLUSION

This paper presented a new construction of almost difference sets via cyclotomy of order 10. Furthermore, we determined the equivalence of the obtained almost difference sets to the known cyclotomic almost difference sets having the same parameters up to complementation.

Based on the findings, a single cyclotomic class can produce almost difference sets with parameters (31, 3, 0, 24), (71, 7, 0, 28), and (151, 15, 1, 90). While a single cyclotomic class together with zero can generate an almost difference set with parameters (11, 2, 0, 8), (31, 4, 0, 18), (71, 8, 0, 14), and (151, 16, 1, 90). We have also found a $(q, (q-3)/2, (q-7)/4, q-3)$ almost difference sets in $GF(q)$ from unions of cyclotomic classes of order 10, where $q = 11$. The obtained $(11, 4, 1, 8)$ almost difference set can generate sequences of period $q \equiv 3 \pmod 4$ with optimal correlation values -1 and 3, where $k = 4$. We have constructed a $(q, (q-1)/2, (q-5)/4,\ (q-1)/2)$ almost difference sets in $GF(q)$ from the union of five cyclotomic classes of order 10, where $q \equiv 1\ (mod\ 4)$. This set can generate sequences of period $q \equiv 1 \pmod 4$, where $k = (q-1)/2$. These two results are open problems (Nowak, 2014). Similarly, a $(q, (q+1)/2, (q-1)/4,\ (q-1)/2)$ almost difference set is also constructed from the union of five cyclotomic classes of order ten together with zero, where $q \equiv 1\ (mod\ 4)$. Moreover, there exist two inequivalent $(31, 7, 1, 18)$ almost difference sets, three inequivalent $(31, 9, 2, 18)$ almost difference sets, and two inequivalent $(31, 13, 5, 24)$ almost difference sets. Other almost difference sets are also constructed for $q = 131$ with parameters $(131, 52, 20, 78)$ and $(131, 53, 21, 104)$.

It is still an open problem to generalize and prove the results not just for a range of prime but for all primes of the form $q = 10n + 1$ for any integer $n \geq 1$ using other theoretical methods without computer search.

REFERENCES

Balmaceda, J. M. P., & Estrella, B. M. (2021). Difference sets from unions of cyclotomic classes of orders 12, 20, and 24. *Philippine Journal of Science, 150*(6B), 1803–1810. https://doi.org/10.56899/150.6B.16

Davis, J. A. (1992). Almost difference sets and reversible difference sets. *Archiv Der Mathematik 59*(6), 595–602. https://doi.org/10.1007/BF01194853

Ding, C. (1994). The differential cryptanalysis and design of the natural stream ciphers. In *R. Anderson Fast software encryption: Cambridge security workshop, Cambridge, U.K., December 9-11, 1993 proceedings,* (pp. 101–115). https://doi.org/10.1007/3-540-58108-1

Ding, C. (2014). *Codes from difference sets.* World Scientific. https://doi.org/10.1142/9283

Ding, C., Helleseth, T. & Martinsen, H. M. (2001). New families of binary sequences with optimal three-level autocorrelation. IEEE Trans. *Information Theory, 47*(1), 428–433. https://doi.org/10.1109/18.904555

Ding, C., Pott, A. & Wang, Q. (2014). Constructions of almost difference sets from finite fields. D*esigns, Codes and Cryptography, 72,* 581-592. https://doi.org/10.1007/s10623-012-9789-9

Estrella, B. M. (2022). Construction of difference sets from unions of cyclotomic classes of order N=14. R*ecoletos Multidisciplinary Research Journal, 10*(1), 67-76. https://doi.org/10.32871/rmrj2210.01.04

Nowak, K. (2014, August 30). *A survey on almost difference sets.* arXiv. https://doi.org/10.48550/arXiv.1409.0114

Nowak, K., Olmez, O., & Song, S. Y. (2013, October 4). *Almost difference sets, normally regular digraphs and cyclotomic schemes fom cyclotomy of order twelve*. arXiv. https://doi.org/10.48550/arXiv.1310.1164

How to cite this article:

Estrella, B. (2024). Almost Difference Sets from Unions of Cyclotomic Classes of Order 10. Recoletos Multidisciplinary Research Journal 12(1), 157-168. https://doi.org/10.32871/rmrj2412.01.12